UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,591	07/09/2007	Lior Golan	P-6325-US	3590

80048 7590 04/12/2011

Pearl Cohen Zedek Latzer, LLP
1500 Broadway
12th Floor
New York, NY 10036

EXAMINER
GEORGANDELLIS, ANDREW C

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
04/12/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@pczlaw.com
Arch-USPTO@pczlaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/578,591	GOLAN ET AL.	
	Examiner	Art Unit	
	ANDREW GEORGANDELLIS	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 February 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Introduction

1. Claims 1-34 are pending. Claims 1, 2, 8, 15, 23, 24, 30, and 32 are amended. No claims are cancelled. No new claims are added. This Office Action is in response to Applicant's request for reconsideration after non-final rejection filed on 2/10/2011.

Response to Arguments

2. Applicant's arguments are unpersuasive for the reasons provided below.

3. Priority claim

4. In the previous Office Action, Examiner indicated that several of the claimed features are not supported in the provision application to which Applicant claims priority. Applicant's response neglects to address Examiner's concerns regarding lack of support in the provisional application.

5. Rejection of claims 1-7, 10, 14, 15, 17, 18, and 24-34 under 35 U.S.C. 101

6. Applicant has amended claims 1-7, 10, 14, 15, 17, 18, and 24-34 to recite a "server processor." Therefore, Examiner withdraws the rejection of claims 1-7, 10, 14, 15, 17, 18, and 24-34 under 35 U.S.C. 101.

7. Rejection of claims 8, 23, and 30 under 35 U.S.C. 112

8. Applicant has amended claims 8, 23, and 30 to clarify that "the set" refers to "the set of data" rather than to "set of false identities." Therefore, Examiner withdraws the rejection of claims 8, 23, and 30 under 35 U.S.C. 112.

9. Rejection of claims 1 and 24 under 35 U.S.C. 103(a)

10. Applicant has amended claim 1 to indicate that the step of responding is performed "by a server" and now argues that NPL does not teach the newly added feature. However, Examiner respectfully disagrees. NPL teaches that a user at a mail client generates a response intended for a scammer and sends the response to a mail server, which in turn forwards the response to the scammer. See NPL, pg. 1-5. By forwarding the user's response to the scammer, the mail server can be said to be responding to the scammer.

11. Assuming arguendo that NPL does not teach that the step of responding is performed by a server, Shraim teaches a method of automatically responding to a phishing attack originating from a phishing website whereby a server generates a plurality of responses and transmits the responses to the phishing website. See par. 92-96.

12. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of NPL so that the responses are "by a server" because doing so allows the process of NPL to be automated. See MPEP 2144.04.B.III, which states that "providing an automatic or mechanical means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art."

13. Rejection of claim 2 under 35 U.S.C. 103(a)

14. Applicant has amended claim 2 to recite "responding to a contact point a plurality of times" and now argues that NPL does not teach the newly added feature. However, Examiner respectfully disagrees. As indicated above, NPL teaches that a user attempts to fool a scammer into believing the user is scam victim. To that end, the user engages in a dialogue with the scammer. For instance, NPL teaches that "Kris Kringle" engages in a dialogue with scammer

"Stella Mike." In other words, "Kris Kringle" sends multiple responses to "Stella Mike," each response including a different set of personal details. See NPL, pg. 1-5.

15. Rejection of claims 3, 16, and 25 and under 35 U.S.C. 103(a)

16. Regarding claims 3, 16, and 25, Applicant argues that AAPA "does not cure the deficiencies of NPL discussed above." However, the alleged "deficiencies" of NPL have been addressed above in the context of claim 1.

17. Rejection of claims 4 and 26 under 35 U.S.C. 103(a)

18. Regarding claims 4 and 26, Applicant argues that NPL does not teach that the contact address is an email address. In support of this argument, Applicant argues that NPL teaches that the contact address is a fax number. However, Examiner respectfully disagrees. Clearly, NPL teaches that fake victim "Kris Kringle" corresponds with scammer "Stella Mike" via the email address of "Stella Mike," i.e., "stellamike@mail.com." See pg. 2.

19. Rejection of claims 5, 6, 8, 18, 27, and 28 under 35 U.S.C. 103(a)

20. Regarding claims 5, 6, 8, 18, 27, and 28, Applicant argues that Shraim "does not cure the deficiencies of NPL discussed above." However, the alleged "deficiencies" of NPL have been addressed above in the context of claim 1.

21. Rejection of claims 7 and 29 under 35 U.S.C. 103(a)

22. Regarding claims 7 and 29, Applicant argues that "the details provided by Kris Kringle are obviously not designed to be consistent in any way. For example, Kris Kringle provides a phone number of 613-9833 xxxx. In contrast, the present Application discloses generating responses that include details which are internally consistent and appear to be legitimate." However, there is nothing obviously inconsistent about providing a phone number of 613-9833

xxxx. In fact, Mike Stella clearly believes that Kris Kringle's response is legitimate. Furthermore, there can be no doubt that Kris Kringle intends to appear legitimate.

23. Rejection of claims 11-13, 15, and 31 under 35 U.S.C. 103(a)

24. Regarding claims 11-13, 15, and 31, Applicant argues that NPL does not teach the limitation "by a server." However, the limitation "by a server" has already been addressed in the context of claim 1.

25. Rejection of claim 14 under 35 U.S.C. 103(a)

26. Regarding claim 14, Applicant summarily concludes that "Hertz does not respond with marked data." As such, Examiner refers Applicant to the rejection of claim 14 below.

27. Rejection of claim 17 under 35 U.S.C. 103(a)

28. Regarding claim 17, Applicant argues that Shur "does not cure the deficiencies of NPL discussed above." However, the alleged "deficiencies" of NPL have been addressed above in the context of claim 1.

29. Additionally regarding claim 17, Applicant argues that Shur "is unrelated to a response, rather, to content being distributed." However, Examiner relies upon NPL for the response. Applicant is reminded that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

30. Rejection of claims 19, 22, and 32 under 35 U.S.C. 103(a)

31. Regarding claims 19, 22, and 32, Applicant argues that NPL does not teach that the contact point is a website. However, Examiner relies upon AAPA for a contact point being a

website. Again, Applicant is reminded that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

32. Rejection of claims 20, 21, 23, 33, and 34 under 35 U.S.C. 103(a)

33. Applicant argues that neither AAPA nor Shraim "can cure the deficiencies of the NPL reference." However, the alleged "deficiencies" of NPL have been addressed above in the context of claim 1.

Priority Claim

34. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. However, the disclosure of the prior-filed application, provisional application No. 60/517,858, fails to provide adequate support or enablement in the manner provided by the first paragraph of 35 U.S.C. 112 for one or more claims of this application.

35. Specifically, the provisional application discloses a "system and method" carried out by a "server." See pg. 7, ln. 11. The server detects phishing scams and alerts an Internet Service Provider (ISP) of the detected scam. See pg. 7, ln. 9-14. In response, the ISP can perform "clogging," i.e., the ISP can fill a phishing website with fake records. See pg. 7, ln. 29-31. In addition, the ISP can mark the fake information in order to catch or block the scammer. See pg. 8, ln. 1-13.

36. However, the provisional application is silent as to several of the claimed features:

a. Claims 1, 24, and 32: While the provisional indicates that "clogging" may be performed, the provisional application is silent as to who or what performs the "clogging" appears to be performed by an ISP external to the disclosed server, rather than by the server itself. Even assuming, arguendo that the "clogging" is performed by the server, the provisional does not state the extent to which the server is involved in the "clogging" process. In other words, the provisional is silent as to whether the "clogging" is performed manually by a user operating the server or whether the "clogging" is performed entirely by the server without any human intervention.

b. Claims 5-9, 11-13, 15, 17, 18, 20-23, 27-31, 33, and 34: The provisional is silent as to the rate at which the responses are transmitted, the timing of the responses, the consistency of the personal information, the creation and storage of false identities in a database, conducting the responses using multiple access points, intermediate networks and/or ISPs, generating a number of responses in proportion to the size of the attack, marking the responses using a cryptographic algorithm, and detecting the marking using a cryptographic key.

Claim Rejections: 35 U.S.C. 112

37. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

38. Claims 1, 24, and 32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

39. Claims 1, 24, and 32 recite a method performed "by a server processor, the method comprising: responding, by the server processor, to a contact point created by a party committing fraud...." Does "responding, by the server processor" mean 1) that the server automatically generates the response without human intervention and sends the response to the contact point, 2) that a human uses the server to manually generate and transmit the response to the contact point, or 3) that the response is generated at a client (i.e., an email client), forwarded by the mail client to the server (i.e., a mail server), and forwarded by the server to the contact point?

Claim Rejections: 35 U.S.C. 103

40. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

41. Claims 1-2, 5-13, 15, 18, 24, and 26-31 are rejected under 35 U.S.C. 103(a) because they are unpatentable over Sweetchillisauce (NPL) in view of Shraim (US 2005/0257261).

42. Regarding claims 1, 10, and 24, NPL teaches a method comprising: responding, by a server, to a contact point created by a party committing fraud (A user at a mail client generates a response to a phishing attack by a scammer and forwards the response to a mail server, which in turn forwards the response to the scammer. See NPL, pg. 1-5), the response including a set of details, the set of details including a set of false personal information (The response includes

false personal information intended to lure the scammer into believing the sender is a scam victim. See NPL, pg. 1-5).

43. However, assuming arguendo that NPL does not teach that the response is "by a server," Shraim teaches a method of automatically responding to a phishing attack originating from a phishing website whereby a server generates a plurality of responses and transmits the responses to the phishing website. See par. 92-96.

44. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of NPL so that the responses are "by a server" because doing so allows the process of NPL to be automated. See MPEP 2144.04.B.III, which states that "providing an automatic or mechanical means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art."

45. Regarding claim 2, NPL teaches responding a plurality of times, each response including a different set of details ("Kris Kringle" engages in a dialogue with scammer "Stella Mike." In other words, "Kris Kringle" sends multiple responses to "Stella Mike," each response including a different set of personal details. See NPL, pg. 1-5).

46. Regarding claims 4 and 26, NPL teaches that the contact point is an e-mail address (The contact address of "Stella Mike" is "stellamike@mail.com").

47. Regarding claims 5, 6, 27, and 28, NPL and Shraim collectively teach responding at a speed designed to mimic a human entering data in response to a phishing attack (Shraim teaches a server that generates a plurality of responses to a phishing attack at a rate which varies according to the purpose of the responses. For instance, the responses can be generated at rate

capable of overwhelming the attacker, or the responses can be generated at a rate intended to lead the attacker to believe that the responses are genuine. See pars. 92-96).

48. Regarding claims 7 and 29, NPL teaches that each response includes a set of details that are internally consistent (Kris Kringle attempts to fool Stella Mike into believing Kris Kringle is a real scam victim. As such, it is understood that Kris Kringle's responses are internally consistent so as to appear genuine).

49. Regarding claims 8 and 30, NPL and Shraim collectively teach creating a database including a set of false identities, each false identity including a set of data which is consistent with the set of data (Shraim teaches a safe data store 236, which stores personal information associated with one or more fictitious entities. See par. 23. See also fig. 2, item 236. It may be inferred that the personal information is internally consistent based on the fact that the personal information is used to fool an attacker).

50. Regarding claim 9, NPL teaches that each response includes a set of details consistent with an Internet service provider used to respond (The responses include details regarding the service providers from which they originate. For instance, a response sent from ISP "America Online" is sent from the domain "aol.com").

51. Regarding claims 11-13 and 31, NPL teaches that the responding is conducted using a plurality of Internet access points and/or intermediate networks and/or Internet service providers (Scam requests are transmitted to multiple users all over the world in order to increase the likelihood of receiving a response. Thus, responses from scam baiters originate from all over the world and are therefore conducted using a variety of networks, access points, and ISPs).

52. Regarding claim 15, NPL teaches that the number of responses is in proportion to a size of an attack in response to which the responses are sent (Each response is generated in response to a scam request. Therefore, the number of responses is correlated with the number of requests. Thus, the greater the number of scam requests sent by "Stella Mike," the greater the number of responses sent by scam baiters such as "Kris Kringle").

53. Regarding claim 18, NPL and Shraim collectively teach that the timing of the sending of the data mimics the behavior of automated client software (Shraim teaches automatically generating a plurality of responses to a Phishing attack at a rate which can be varied depending upon the purpose of the responses. For instance, the responses can be generated at rate capable of overwhelming the attacker, or the responses can be generated at a rate intended to lead the attacker to believe that the responses are genuine. See pars. 92-96).

54. Claims 3, 16, and 25 are rejected under 35 U.S.C. 103(a) because they are unpatentable over NPL and Shraim, as applied to claims 1 and 24 above, in further view of Applicant Admitted Prior Art (AAPA).

55. Regarding claims 3, 16, and 25, NPL does not explicitly teach that the contact point comprises a website or responding comprises entering data into a web-form. However, AAPA teaches responding to a fishing attack that originates from a website by entering data into a web-form of the website. See Specification, pg. 2, par. 2.

56. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of NPL/Shraim so that the responses are submitted by filling in a web-form because doing so allows the responses to be generated in response to a phishing attack originating from a website.

57. Claim 14 is rejected under 35 U.S.C. 103(a) because it is unpatentable over NPL and Shraim, as applied to claim 1 above, in further view of Herz (US 2006/0053490).

58. Regarding claim 14, NPL and Shraim do not explicitly teach that the data in a response is marked, the method comprising monitoring an institution for the use of marked data in an attempted transaction. However, Herz teaches marking an account number or credit card number and monitoring use of the marked account number or credit card number to detect fraudulent use of the marked account number or credit card number. See par. 88.

59. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of NPL/Shraim so that account information included within the responses is marked because doing so would allow the marked account numbers to be used to capture scammers.

60. Claim 17 is rejected under 35 U.S.C. 103(a) because it is unpatentable over NPL and Shraim, as applied to claim 1 above, in further view of Shur (US 6,330,672).

61. Regarding claim 17, NPL and Shraim do not explicitly teach that response is marked using a cryptographic algorithm, such that the marking is detectable only with a suitable cryptographic key. However, Shur teaches inserting cryptographically hidden data into a data stream, such that the hidden data is detectable only via a cryptographic key. See col. 3, ln. 40-67.

62. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of NPL/Shraim to incorporate the above-described feature because doing so facilitates tracking of the marked response.

63. Claims 19-23 and 32-34 are rejected under 35 U.S.C. 103(a) because they are unpatentable over NPL in view of Shraim and AAPA.

64. Regarding claims 19 and 32, NPL teaches a server processor to contact a plurality of times a contact point and, with each contact, enter a set of data (A user at a mail client generates a plurality of responses to a phishing attack by a scammer and forwards the responses to a mail server, which in turn forwards the response to the scammer. See NPL, pg. 1-5), each set of data including a set of details, the set of details including a set of false personal information (The responses each include false personal information intended to lure the scammer into believing the sender is a scam victim. See NPL, pg. 1-5).

65. However, assuming arguendo that the method of NPL is not performed by a "server processor," Shraim teaches a method of automatically responding to a phishing attack originating from a phishing website whereby a server generates a plurality of responses and transmits the responses to the phishing website. See par. 92-96.

66. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of NPL so that the responses are "by a server" because doing so allows the process of NPL to be automated. See MPEP 2144.04.B.III, which states that "providing an automatic or mechanical means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art."

67. In addition, NPL does not explicitly teach that the contact point is a website, and that responding comprises entering data into a web-form. But AAPA teaches responding to a fishing attack that originates from a website by entering data into a web-form of the website. See Specification, pg. 2, par. 2.

68. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of NPL/Shraim so that the responses are submitted by filling in a web-form

because doing so allows the responses to be generated in response to a phishing attack originating from a website.

69. Regarding claims 20, 21, and 34, NPL and Shraim collectively teach responding at a speed designed to mimic a set of unrelated human users entering data in response to a phishing attack (Shraim teaches a method of automatically responding to a phishing attack originating from a phishing website whereby a server generates a plurality of responses and transmits the responses to the phishing website at a rate which varies according to the purpose of the responses. For instance, the responses can be generated at rate capable of overwhelming the attacker, or the responses can be generated at a rate intended to lead the attacker to believe that the responses are genuine. See pars. 92-96).

70. Regarding claim 22, NPL and AAPA collectively teach that each contact includes a set of details that are internally consistent (The scam baiter attempts to fool the scammer into believing the response is genuine. Therefore, it may be inferred that the set of details in the response are internally consistent in order to make the response appear genuine).

71. Regarding claims 23, NPL and Shraim collectively teach creating a database including a set of false identities, each false identity including a set of data which is consistent with the set (Shraim teaches a safe data store 236, which stores personal information associated with one or more fictitious entities. See par. 23. See also fig. 2, item 236. It may be inferred that the personal information is internally consistent based on the fact that the personal information is used to fool an attacker).

72. Regarding claim 33, NPL and Shraim collectively teach creating a database including a set of false identities (Shraim teaches a safe data store 236, which stores personal information associated with one or more fictitious entities. See par. 23. See also fig. 2, item 236).

Conclusion

73. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

74. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

75. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew Georgandellis whose telephone number is (571)270-3991. The examiner can normally be reached on Monday through Friday, 7:30-5:00 PM EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele can be reached on 571-272-7288. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

76. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW GEORGANDELLIS/
Examiner, Art Unit 2453

/Krista M. Zele/
Supervisory Patent Examiner, Art Unit 2453